ARTICLE APPEARED ON PAGE A-9
THE WASHINGTON TIMES
31 AUGUST 1982

JOHN A. WETTERGREEN

Industrial espionage: the stakes are high

The indictment of 17 employees of Hitachi and Mitsubishi for industrial espionage against IBM has drawn wide attention.

And rightly so. For the case pits the commerical honor of Japan against the technological superiority of the U.S.

But ultimately the matter involves more than our commercial interest as against that of our industrial rival. Our military advantage, as against that of our deadly enemies, is also at stake.

Industrial espionage is a special problem for the electronics industry just now, because that industry is closely competitive, rapidly growing, and very profitable. A lead of just a few months in the design, production, or marketing of the latest electronic device can mean tens or even hundreds of millions in profits. Thus, otherwise respectable electronics companies have been caught trying to acquire not only information about their rivals' plans, but also their competitors' prototypes, products, and tools of design, testing, and production. At the extreme, some companies have been willing to sabotage others' operations.

Even small electronics firms, and even firms not engaged in production for high-tech weaponry (such as that used by Israel to defeat the Syrians' Soviet-supplied airforce) take extraordinary security precautions. The largest, most innovative firms go far beyond the usual armed guards, plant passes, electronic surveillance, alarms, and fences. IBM, for example, employs several former CIA officers, at very high salaries, to superintend the secrecy of its plants and employees. Nevertheless, IBM is "penetrated" often — so often, it is rumored, that the company's managers have to decide which cases are worthy of prosecution.

John Wettergreen is a professor of political science at San Jose State University in California.

Security measures, however rigorous, have not prevented the development of international black markets for electronics devices and information. These markets greatly benefit some electronics companies in their struggle with their competitors. More important, though, these markets benefit the Soviets' GRU (military intelligence agency).

Recently, the Commerce Department leaked the news that some information and goods pirated in the U.S. for commercial advantage end up in the hands of Soviet agents in Tokyo. The GRU is also reported to be active in the black and grey markets of Taiwan, Hong Kong, Singapore, Thailand, Los Angeles, and San Jose, California.

The Soviet Union is not the only one of our potential military enemies involved in industrial espionage. Chipex, a tiny electronics firm in the Silicon Valley, was recently alleged in fact to be a Communist Chinese front. Moreover, an FBI investigation at General Electric in San Jose indicates that the Mainland Chinese are involved in an international high-tech counterfeiting ring.

But it is Moscow that is most active on the industrial espionage front. Because they have a highly centralized, minutely pervasive intelligence operation the Soviets can take advantage of even small lapses in security. Legitimate Soviet businesses employ GRU agents: in the past six months alone, 19 employees of Aeroflot, the Soviet commercial airline, have been expelled from 11 countries for spying. Soviet allies serve the GRU in the same way: an East German importer of washing machines was found to be shipping sensitive electronics testing devices to the Soviets. Nor is it any accident that the Soviet Consulate in San Francisco aims its elaborate listening devices at the telephone lines of the Silicon Valley, 40 miles south, which abounds in high-tech companies.

The black markets of industrial espionage aid our foes by supplying them with technology they cannot themselves produce and with information about our weaponry. But industrial espionage can also do us positive harm. For where there is the exchange of pirated goods and information, there is also the potential for sabotage. For example, the reliability of computer chips bought on the black market is no more likely to be checked than their point of origin. Yet those chips could well end up in a weapon used by an American soldier.

The size of the industrial espionage problem and the degree of Soviet participation in it are difficult to calculate. Recent investigations concerning $2 million in chips stolen from Advanced Microdevices and $3.2 million funneled through Brut Electronics revealed the usual American underworld connections. But also revealed was the indirect involvement of a Soviet agent. It should be noted, though, that these and similar cases are instances of failure on the part of spies and thieves. Successful acts are seldom reported.

This much can be said: if industrial espionage were only a matter of commercial advantage, then it would not be a serious problem. As the electronics industry develops, shortages of products and information will decline, and the competitive edge will become less important. However, in the present circumstances, industrial espionage — even for the narrowest commercial advantage — amounts to a betrayal of Western security.